REMARKS

This is in response to the Final Office Action dated April 5, 2004. Claims 1 to 34 are pending. The Examiner's reconsideration of the rejections is respectfully requested in view of the remarks.

Claims 1, 2, 4-13, 16-20, 22-26, 28-31, 33, and 34 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa (U.S. Patent No. 5,872,846) in view of Orrin (U.S. Patent No. 6,011,849). The Examiner stated essentially that the combined teachings of Ichikawa and Orrin teach or suggest all the limitations of claims 1, 2, 4-13, 16-20, 22-26, 28-31, 33, and 34.

Claim 1 claims, *inter alia*, "a scrambler for encrypting at least one first unit using an encryption key; a steganographic unit for embedding the encryption key into at least one second unit for the data stream." Claims 20 and 33 recite, *inter alia*, "scrambling at least one first unit by encrypting the at least one first unit using an encryption key; and steganographically embedding the encryption key into at least one second unit for the data stream."

Ichikawa teaches a dual key encryption method/system comprising a public key and a private key (see Figures 5 and 6). Ichikawa teaches a dual key encryption method, wherein two sets of asymmetric keys are implemented, one used for encrypting data and another used to encrypt a user's public key (see Figure 6 and col. 5 lines 44-64). Ichikawa does not teach or suggest "encrypting at least one first unit using an encryption key" and "embedding the encryption key into at least one second unit for the data stream" essentially as claimed in claims 1, 20, and 33 (Emphasis added). Ichikawa teaches that a sender encrypts data using a receiver's public key (see Figure 5). The receiver's public key is previously delivered to the sender in encrypted form, wherein the receiver used the sender's public key to encrypt the receiver's

public key (see Figure 6). The user in Figure 6 of Ichikawa is the sender shown in Figure 5. Thus, the key used for performing the encryption of data is different from the key encrypted and delivered to the sender. Ichikawa does not teach or suggest encrypting, much less embedding, an encryption key in a second unit of a data stream that was used to encrypt a first unit of the data stream. Therefore, Ichikawa fails to teach or suggest "embedding the encryption key into at least one second unit for the data stream" as claimed in claims 1, 20, and 33.

Orrin teaches a method wherein an encryption key is used as a key and data to be encrypted (see col. 4, lines 45-64). Orrin teaches that data is encrypted using a Pseudo Random Number Generator (PRNG) generated session key to create message ciphertext, and that the session key is then encrypted using a recipient's public key, the encrypted session key being added to a header of the message ciphertext (see col. 7, lines 59-65). Thus, the session key is not embedded into at least one second unit, essentially as claimed in claims 1, 20, and 33. The session key of Orrin is merely encrypted using the recipient's public key and added to a header (see col. 7, lines 59-65). According to Orrin, the data in, which is encrypted (see col. 4, lines 13-17) and steganographically encoded (see col. 4, lines 34-44), is treated distinctly from the session key, which is encrypted and added to a header (see col. 7, lines 59-65). The session key of Orrin is used as a key and data to be encrypted (see col. 4, lines 45-64). Nowhere does Orrin teach or suggest that the session key is steganographically encoded. Therefore, Orrin does not teach or suggest "encrypting at least one first unit using an encryption key" and "embedding the encryption key into at least one second unit for the data stream" essentially as claimed in claims 1, 20, and 33. Therefore, Orrin fails to cure the deficiencies of Ichikawa.

Referring now to claims 8, 26, and 34: claim 8 recites, *inter alia*, "a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream

received from the server." Claims 26 and 34 claim, *inter alia*, "extracting an encryption key steganographically embedded in at least one second unit in the data stream."

As suggested by the Examiner, Ichikawa does not teach a system or method of a server comprising a steganographic unit for embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by the client to determine the encryption key and decipher the data stream. Thus, Ichikawa does not teach or suggest "extracting an encryption key steganographically" hidden or embedded in a unit of a data stream, essentially as claimed in claims 8, and 26 and 34, respectively. Therefore, Ichikawa fails to teach or suggest each limitation of claims 8, 26, and 34.

Orrin teaches a method wherein an encryption key is used as a key and data to be encrypted (see col. 4, lines 45-64). Orrin teaches that data is encrypted using a Pseudo Random Number Generator (PRNG) generated session key to create the message ciphertext, and that the session key is then encrypted using a recipient's public key, the encrypted session key being added to a header of the message ciphertext (see col. 7, lines 59-65). Orrin does not teach or suggest "a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream" as claimed in claim 8, or "extracting an encryption key steganographically embedded in at least one second unit in the data stream" as claimed in claims 26 and 34. The session key of Orrin is encrypted using the recipient's public key and added to a header (see col. 7, lines 59-65). Nowhere does Orrin teach or suggest a steganographically hidden session key, much less the extraction of a steganographically hidden session key. Encryption of a session key using a public key as taught by Orrin is distinct from steganographically extracting an encryption key, essentially as claimed in claims 8, 26 and 34. Therefore, Orrin does not teach or suggest "extracting an encryption key steganographically"

hidden or embedded in a unit of a data stream, essentially as claimed in claims 8, and 26 and 34, respectively. Therefore, Orrin fails to cure the deficiencies of Ichikawa.

Claims 2, and 4-7 depend from claim 1. Claims 9-13 depend from claim 8. Claims 16-19 depend from claim 14. Claims 22-25 depend from claim 20. Claims 28-31 depend from claim 26. The dependent claims are believed to be allowable for at least the reasons given for claims 1, 8, 20, and 26 respectively. Claims 16-19 are believed to be allowable for at least the reasons given for claim 14 below. The Examiner's reconsideration of the rejection is respectfully requested.

Claims 3, 9, 14,15, 21, 27, and 32 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa in view of Orrin and further in view of Katta et al. (U.S. Patent No. 5,621,799).

Claim 14 recites, *inter alia*, "segmenting the data into units for a data stream to be transferred over the link; scrambling at least one first unit by encrypting the at least one first unit using an encryption key; steganographically embedding the encryption key into at least one second unit for the data stream." Claim 32 claims, *inter alia*, "scrambling at least one first unit for the data stream before transmission by encrypting the at least one first unit using an encryption key; steganographically embedding the encryption key into at least one second unit for the data stream."

Ichikawa teaches a dual key encryption method, wherein two sets of asymmetric keys are implemented, one used for encrypting data and another used to encrypt a user's public key (see Figure 6 and col. 5 lines 44-64). Ichikawa teaches asymmetric key encryption. Nowhere does Ichikawa teach or suggest a steganographic method/system. Therefore, Ichikawa does not teach or suggest "steganographically embedding the encryption key into at least one second unit for the data stream" as claimed in claims 14 and 32.

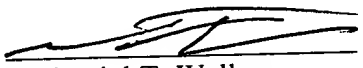
Orrin teaches that data is encrypted using a Pseudo Random Number Generator (PRNG) generated session key to create the message ciphertext, and that the session key is then encrypted using a recipient's public key, the encrypted session key being added to a header of the message ciphertext (see col. 7, lines 59-65). The session key of Orrin is encrypted using the recipient's public key and added to a header (see col. 7, lines 59-65). Nowhere does Orrin teach or suggest that the session key is embedded. Therefore, Orrin does not teach or suggest "steganographically embedding the encryption key into at least one second unit for the data stream" as claimed in claims 14 and 32. Thus, Orrin fails to cure the deficiencies of Ichikawa.

Katta teaches a system for transmitting digital data containing variable length coding comprising a first scramble key generating means for generating a first scramble key at a first predetermined interval; a second scramble key generation means for generating a second scramble key based on said first scramble key at a second predetermined interval smaller than said first predetermined interval; a scrambling means for scrambling said digital data based on said second scramble key (see col. 2, lines 30-45). Katta does not teach or suggest "steganographically embedding the encryption key into at least one second unit for the data stream" as claimed in claims 14 and 32. Katta teaches the digital data to be scrambled has a variable length encoding. Katta does not teach or suggest "steganographically embedding the encryption key into at least one second unit for the data stream" as claimed in claims 14 and 32. Therefore, Katta fails to cure the deficiencies of Ichikawa and Orrin.

Claim 3 depends from claim 1. Claim 9 depends from claim 8. Claim 15 depends from claim 14. Claim 21 depends from claim 20. Claim 27 depends from claim 26. The dependent claims are believed to be allowable for at least the reasons given for the independent claims. The Examiner's reconsideration of the rejection is respectfully requested.

Accordingly, claims 1 to 34 are believed to be allowable for at least the reasons stated. For the forgoing reasons, the application, including claims 1 to 34, is believed to be in condition for allowance. Early and favorable reconsideration of the rejections is respectfully requested.

Respectfully submitted,



Nathaniel T. Wallace
Reg. No. 48,909
Attorney for Applicants

F. CHAU & ASSOCIATES, LLC
1900 Hempstead Turnpike, Suite 501
East Meadow, New York 11554
(516) 357-0091
(516) 357-0092 (FAX)